CLAIMS

ADD A37

1. A method of controlling the use of a smart card comprising a microprocessor able to effect cryptography calculations in the card for effecting authentication sessions at the time of a transaction between the card and a terminal, characterised in that the said method uses at least one control counter (C_{KDP}) and in that, for a transaction comprising at least one authentication session by the card, the method consists of:

- decrementing or incrementing the control counter by one unit (u) at the start of the transaction, and

- if the authentication by the card has succeeded, effecting the reincrementation or decrementation of the said control counter by the said unit (u).

2. A method according to Claim 2, characterised in that the control counter can count down from or count up to a blocking value.

3. A method according to Claim 2, characterised in that it comprises the use of a control counter by an encrypting key and/or by a pair of encrypting keys contained in the card.

4. A method according to Claim 3, characterised in that the blocking value associated with a counter is a function of the type of transaction in which the associated key or the associated pair of keys is used.

5. A method according to Claim 3, characterised in that the decrementation or incrementation unit of a control counter represents the number of cryptographic

calculations with the associated key or the associated pair of keys, performed up till then and including the one consisting of the said authentication session during the said transaction.

6. A method according to Claim 3, characterised in that the control counter associated with a key or a pair of keys is decremented or incremented by a new unit before each of the cryptographic calculations using the said key or the said pair of keys up to and including the one relating to the said authentication session by the card.

7. A method according to Claim 5, characterised in that the reincrementation or decrementation of the counter by the unit representing the number of cryptographic calculations is effected if the authentication session by the card has succeeded.

8. A method according to Claim 6, characterised in that it comprises a pointing counter (D_{KDP}) for storing the number of decrementations or incrementations by one unit carried out, to permit the reincrementation or decrementation of the control counter (C_{KDP}) via the content of the pointing counter, if the authentication session by the card has succeeded.

9. A control method according to any one of the preceding claims, characterised in that the said authentication session by the card is effected at the time of a connection by direct link to a server.

10. A method according to any one of the preceding claims, characterised in that, when the

control counter is decremented, or incremented, up to a limit value, it blocks the use of the associated key or associated pair of keys.

11. A method according to Claim 10, characterised in that the blocking of the use of the key or pair of keys is irreversible.

12. A smart card comprising at least one control counter associated with at least one key and/or one pair of keys for implementing a control method according to any one of the preceding claims.

ADD A2 (ABSTRACT)